

*Религиозная организация
Образовательная организация
высшего образования
Духовная Академия «Благодать»
христиан веры евангельской*

Приказ

29.08.2018 г.

№ 49/18

г. Москва

(О принятии и введении в действие локальных актов)

На основании решения Ученого совета (Протокол заседания № 4/18 от 28.08.2018 г.)

Приказываю:

1. Принять следующие локальные акты:

- 1) Положение об электронной информационно-образовательной среде (ЭИОС)
- 2) Положение об электронном обучении
- 3) Положение о парольной политике Религиозной организации Образовательной организации высшего образования духовной Академии «Благодать» христиан веры евангельской

2. Ввести в действие данные локальные акты с 01.09.2018 г.

Ректор



Князев Н.Н.

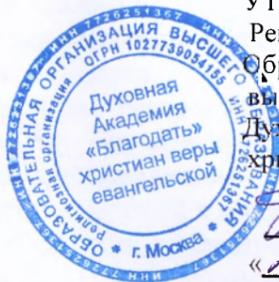
Визы:
Академический декан

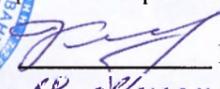


Князева Е.М.

**Религиозная организация
Образовательная организация высшего образования
Духовная Академия «Благодать»
христиан веры евангельской**

ПРИНЯТО
На заседании Ученого совета
Религиозной организации
Образовательной организации
высшего образования
Духовная Академия «Благодать»
христиан веры евангельской
Протокол № 4/18
от 18 августа 2018 г.



УТВЕРЖДАЮ
Ректор Религиозной организации
Образовательной организации
высшего образования
Духовной Академии «Благодать»
христиан веры евангельской

Князев Н.Н.
«18» августа 2018 г.

**ПОЛОЖЕНИЕ
О парольной политике**

Москва, 2018 г.

1. Общие положения

1.1. Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями в Религиозной организации образовательной организации высшего образования Духовной Академии «Благодать» христиан веры евангельской (далее- Академия).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Академии.

1.3. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Академии.

1.4. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети Академии) и должны применяться для всех средств вычислительной техники, эксплуатируемой в Академии.

1.5. Ознакомление всех работников Академии, использующих средства вычислительной техники, с требованиями положения проводит администратор ИБ. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.

1.6. Термины и определения:

➤ Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений. К автоматизированным системам относятся также компоненты электронной информационно-образовательной среды.

➤ Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности бизнеса, минимизации рисков бизнеса и максимального увеличения возможностей бизнеса.

➤ Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа. Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе.

➤ Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

➤ Принцип минимальных привилегий - принцип, согласно которому «каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

➤ Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

➤ Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

2. Общие требования к паролям

2.1. Пароли доступа ко всем подсистемам АС Академии, информационным ресурсам первоначально формируются администратором ИБ, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

2.2. Личные пароли пользователей автоматизированной системы Академии должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, \$, &, *, % и т.п.). Исключение составляют подсистемы АС Академии, в которых использование подобных спецсимволов недопустимо;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa\$\$w0rd, и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами.

2.3. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать, цифры и (или) специальные символы (@, #, \$, &, *, % и т.п.). Исключение составляют подсистемы АС Организации, в которых использование подобных спецсимволов недопустимо;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa\$\$w0rd, и т.п.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0, s->\$, a->@ и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд;
- при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей.